

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problems Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-143556

(43) 公開日 平成10年(1998) 5月29日

(51) Int.Cl.<sup>6</sup>

G 0 6 F 17/60

識別記号

F I

G 0 6 F 15/21

3 4 0 B

審査請求 未請求 請求項の数 3 O L (全 8 頁)

(21) 出願番号

特願平8-298826

(22) 出願日

平成8年(1996)11月11日

(71) 出願人 393007868

株式会社ユーカード

東京都渋谷区元代々木町30-13

(72) 発明者 落合 祐二

東京都渋谷区元代々木町30-13 日交元

代々木ビル 株式会社ユーカード内

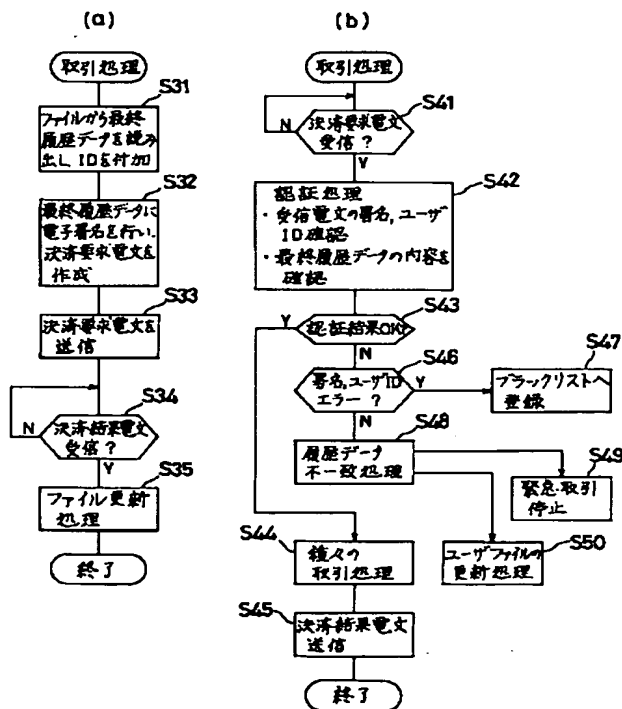
(74) 代理人 弁理士 山川 政樹

(54) 【発明の名称】 電子決済システムにおける利用者限定方法

(57) 【要約】

【課題】 電子商取引を行う場合に高セキュリティを確保する。

【解決手段】 ネットワーク13を介した電子商取引における決済時には、ユーザ端末11はユーザファイル12内の最終履歴データを管理センタ14へ送信し、管理センタ14ではこのデータを受信してデータベース42内のユーザ端末11に対応する最終履歴データとの一致を確認することでその決済を許容する。この結果、電子商取引を行う場合にその利用者を限定することができ、従って高セキュリティを確保できる。



## 【特許請求の範囲】

【請求項1】 ネットワークと、ネットワークに接続されると共にデータベースを有し各ユーザの残高の管理を行う残高・ユーザ管理センタと、ネットワークに接続され各ユーザがそれぞれ用いる各端末と、各端末に設けられ各ユーザの取引履歴情報を各個に記録するユーザファイルとからなり、残高・ユーザ管理センタでは、ユーザの電子商取引に伴う決済の都度、前記データベース内の対応のユーザのファイルの残高を更新し、かつこの更新情報を端末側へ送信して前記ユーザファイルを更新する電子決済システムであって、前記電子商取引に伴う決済時に前記端末は前記ユーザファイルの最終履歴情報を前記残高・ユーザ管理センタに送信し、前記残高・ユーザ管理センタはこのユーザファイルの最終履歴情報と前記データベースの最終履歴情報とが一致するときに前記決済を許容することを特徴とする電子決済システムにおける利用者限定方法。

【請求項2】 請求項1において、予めバックアップファイルを前記端末に設けて取引履歴情報をバックアップすると共に、前記残高・ユーザ管理センタからユーザファイルの最終履歴情報とデータベースの最終履歴情報との不一致が通知された場合、前記端末は前記バックアップファイルの取引履歴情報を残高・ユーザ管理センタへ送信しユーザファイルを更新することを特徴とする電子決済システムにおける利用者限定方法。

【請求項3】 請求項1において、前記残高・ユーザ管理センタは履歴情報に自身の署名鍵を用いて電子署名を行い前記端末へ送信してユーザファイルに記録させ、前記端末はユーザファイル内の履歴情報に自身のIDを付加すると共にIDが付加された履歴情報に自身の署名鍵を用いて電子署名を行い前記残高・ユーザ管理センタへ送信し、履歴情報の正否を検証させることを特徴とする電子決済システムにおける利用者限定方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、電子決済システムにおける利用者限定方法に関する。

## 【0002】

【従来の技術】 マルチメディア技術の進歩やインターネット等のネットワークの普及により、電子商取引（エレクトロニック・コマース）が現実化しつつある。こうしたネットワークを介して各ユーザが電子商取引を行う場合、各ユーザの残高の管理を行う残高・ユーザ管理センタをネットワークに接続すると共に、各ユーザでは取引履歴を記録するユーザファイルを各個に設け、残高・ユーザ管理センタでは、ユーザの取引に伴う決済の都度、対応のユーザのファイルの残高を更新し、かつこの更新情報をユーザ側へ送信してユーザファイルを更新させる

ような電子決済システムが検討されている。

## 【0003】

【発明が解決しようとする課題】 こうした電子決済システムではインターネット等のネットワークを介在して不特定多数間で電子商取引が行われるため、他人に勝手に利用される恐れがあり、従って本人認証等のセキュリティには万全の体制をとることが要望されている。従って本発明は、電子決済システムにおいて高セキュリティを確保することを目的とする。

## 10 【0004】

【課題を解決するための手段】 このような課題を解決するために本発明は、ネットワークと、ネットワークに接続されると共にデータベースを有し各ユーザの残高の管理を行う残高・ユーザ管理センタと、ネットワークに接続され各ユーザがそれぞれ用いる各端末と、各端末に設けられ各ユーザの取引履歴情報を各個に記録するユーザファイルとからなり、残高・ユーザ管理センタでは、ユーザの電子商取引に伴う決済の都度、データベース内の対応のユーザのファイルの残高を更新し、かつこの更新情報を端末側へ送信してユーザファイルを更新する電子決済システムであって、電子商取引に伴う決済時に端末はユーザファイルの最終履歴情報を残高・ユーザ管理センタに送信し、残高・ユーザ管理センタはこのユーザファイルの最終履歴情報とデータベースの最終履歴情報とが一致するときに上記決済を許容するようにした方法である。従って、電子商取引を行う場合にその利用者を限定することができ、その結果高セキュリティを確保できる。また、予めバックアップファイルを端末に設けて取引履歴情報をバックアップすると共に、残高・ユーザ管理センタからユーザファイルの最終履歴情報とデータベースの最終履歴情報との不一致が通知された場合、端末はバックアップファイルの取引履歴情報を残高・ユーザ管理センタへ送信しユーザファイルを更新するようにした方法である。従って、ユーザファイル内の履歴データの紛失や破損等が生じた場合でもこれを復旧して決済を行うことができる。また、残高・ユーザ管理センタは履歴情報に自身の署名鍵を用いて電子署名を行い端末へ送信してユーザファイルに記録させ、端末はユーザファイル内の履歴情報に自身のIDを付加すると共にIDが付加された履歴情報に自身の署名鍵を用いて電子署名を行い残高・ユーザ管理センタへ送信し、履歴情報の正否を検証させるようにした方法である。従って、電子決済システムにおいてより高いセキュリティ性を確保できる。

## 【0005】

【発明の実施の形態】 以下、本発明について図面を参照して説明する。図1は本発明を適用した電子決済システムの構成を示すブロック図である。同図において、11A～11Dは電子商取引時に各ユーザA～Dが各個に使用するユーザ端末、12A～12Dは各ユーザ端末11A～11Bに接続され、ユーザの取引履歴情報を記録す

## 3

るユーザファイル、13はインタネット等のネットワーク、14は残高・ユーザ管理センタ（以下、管理センタ）である。管理センタ14には、管理装置41とデータベース42とが設けられ、データベース42には各ユーザA～Dの取引履歴情報が各個に記録されるファイルが設けられている。

【0006】図2はユーザファイル12の構成を示す図であり、上述した取引履歴情報21と署名鍵（電子印鑑）22とを格納する領域を有している。ここで、ユーザファイル12に記録される履歴情報21としては、管理センタ14の図示しない署名鍵により電子署名されたものが記録される。また、署名鍵22は、電子商取引時にユーザ端末11から管理センタ14へ送信される電文に電子署名を行うときに用いられる。

【0007】さて、以上のように構成された電子決済システムの動作の概略を説明する。電子商取引において決済を行うためには、まず正当なユーザであることを確認する必要がある。このため、管理センタ14に対して決済要求を行う場合は、ユーザ認証用の電文が必要になる。ユーザ認証用の電文には、ユーザ個々に与えられるIDと前回利用したときに管理センタ14から受信した上述の電子署名付履歴情報21とが含まれる。そしてその電文全体に対して署名鍵22により電子署名を行い、例えばユーザ端末11Aからネットワーク13を介し管理センタ14へ送信する。

【0008】すると、管理センタ14の管理装置41は、このユーザ認証電文を受信してユーザIDを確認する。また、ユーザの電子署名も図示しない検証鍵により検証する。そして、ユーザID及びユーザの電子署名が正常なものと認識すると、次にデータベース42内のそのユーザに対応するファイルから最終履歴情報を読み出し、受信電文と比較することにより、受信したユーザ認証電文の履歴情報を確認する。そして確認結果が正常な場合、管理装置41は、ユーザによる種々の電子商取引に伴う決済を許可する。

【0009】こうしてユーザにより種々の電子商取引が行われかつその決済時点で依然としてそのユーザに残高があることを確認すると、管理装置41は、この新たな残高情報に対し署名鍵による電子署名を施して最終履歴情報としてデータベース42内の対応するファイルに記録し、かつその最終履歴情報をネットワーク13を介して該当ユーザ端末11Aに送る。この結果、該当ユーザ端末11Aが対応するユーザファイル12Aにその最終履歴情報を記録することにより、ユーザファイル12Aの履歴情報が更新され、次の決済時には更新された新たな最終履歴情報がユーザ端末11Aから管理センタ14へ送信される。

【0010】ところで、こうした電子決済システムでは、ネットワークを介して不特定多数間で電子商取引が行われるため、他人に勝手に利用される恐れがある。図

## 4

3はこうした不正利用の場合の状況を示す図であり、この図は、例えばユーザAが使用するユーザファイル12AをユーザBが不正にコピーしてユーザ端末11Bから決済を行う場合を示している。

【0011】この場合、コピーされたユーザファイル12Aの最終履歴情報は履歴状態であるとする。また、ユーザBが不正使用する前にユーザAが先に自身のユーザファイル12Aを使用してステップS1で決済要求を行うものとする。この決済要求時には履歴状態の履歴情報が最終履歴情報としてネットワーク13を介し管理センタ14に送られる。この場合、管理センタ14の管理装置41は、ステップS2でこの最終履歴情報の認証を行い、その認証結果を正常と認識すると、種々の電子商取引に伴う決済を許可し、決済終了後にはデータベース41内のユーザA用のファイルの履歴状態をステップS3で更新し、ステップS4で履歴状態とする。

【0012】その後、ステップS5でネットワーク13を介してユーザ端末11Aに対し決済結果を通知する。この決済結果としては、履歴状態がユーザ端末11Aに送られ、ユーザファイル12Aの内容が履歴状態から履歴状態に書き換えられる。こうして先にユーザAが決済を行った後、ユーザAのファイル12Aを不正コピーしたユーザBによる決済要求がユーザ端末11BにおいてステップS6で行われるものとする。即ち、ユーザAのコピー情報にそのユーザAのIDを付加すると共にこれらの情報に対し、不正コピーしたユーザAの署名鍵22により電子署名を行い決済要求として管理センタ14へ送信される。この場合、最終履歴情報として履歴状態の履歴情報がネットワーク13を介し管理センタ14に送られることになる。管理センタ14の管理装置41は、ステップS7でこの最終履歴情報の認証を行うが、このときデータベース42内の最終履歴情報は履歴状態となっているため、ステップS8で履歴不一致通知をユーザ端末11Bに対して行う。その結果、他のユーザのファイル12を不正コピーしたユーザBによる決済を禁止することができる。

【0013】また、ユーザAがユーザBのファイル12Bを不正コピーして先に決済を行って管理センタ14内のデータベースの履歴状態をからへ更新した後、ユーザBが決済を行うと、ユーザBの決済行為も同様に禁止される。しかし、このときユーザBは自身のファイル12Bが不正使用されたことに気づきその使用不可の措置を講ずることができる。また、ユーザBが自身の使用するファイル12Bの破壊等により、決済要求時に最終履歴情報が管理センタ14に伝達されず、管理センタ14からステップS8で履歴不一致通知が行われ、従って決済行為が不可となる場合は、ステップS9で履歴の更新を行うことにより、履歴状態をステップS10で履歴状態にすることができる。

【0014】即ち、図4に示すように、ユーザBの使用

## 5

するユーザファイル12Bの履歴情報が最初の履歴状態から最終の履歴状態まで更新されるような場合、ユーザ端末11Bではバックアップファイル15Bに例えば最初の履歴情報(履歴状態)をバックアップしておく。ここでユーザファイル12Bが破壊され、上述の履歴不一致が管理センタ14から通知されると、ステップS21でバックアップファイル15Bから最初の履歴情報を読み出し、ステップS22でユーザ端末11Bから管理センタ14へ送信する。

【0015】すると、管理センタ14の管理装置41では、ステップS23でこの電文に含まれる電子署名の認証等を行い、ステップS24で認証結果が正常となると、データベース42内のユーザBに対応する最終履歴情報を示す履歴状態をステップS25で取り出し、ステップS26で履歴の更新情報として該当ユーザ端末11Bへ送信する。この結果、ユーザファイル12Bには履歴状態が最終履歴情報として記録されることから、以降、ユーザファイル12Bを用いた決済が可能になる。

【0016】図5はこの電子決済システムの動作を示すフローチャートである。このフローチャートに従って本システムの要部動作を説明する。なお、図5(a)はユーザ端末11の動作を、図5(b)は管理センタ14の動作をそれぞれ示している。商品取引時に例えばユーザAがユーザ端末11Aを用いて決済を行う場合は、まず図5(a)のステップS31でユーザ端末11Aはユーザファイル12Aから最終履歴データ(最終履歴情報21)を読み出し、これにユーザIDを付加する。

【0017】次にIDが付加された最終履歴データにステップS32で署名鍵22による電子署名を行い決済要求電文として作成する。そしてステップS33でこの決済要求電文をネットワーク13を介して管理センタ14へ送信する。その後、管理センタ14では上述したように、送信した決済要求電文の認証処理等が行われ、認証結果が正常となると種々の商取引に伴う決済時の残高情報等を決済結果電文としてユーザ端末11A側に送信する。ユーザ端末11AではステップS34でその決済結果電文の受信の有無を判断し、管理センタ14からの決済結果電文を受信すると、その電文をユーザファイル12Aに記録するファイル更新処理をステップS35で実行する。

【0018】一方、こうしたユーザ端末11Aの動作に応動する管理センタ14では、ユーザ端末11Aから送信される決済要求電文の受信の有無を図5(b)のステップS41で判断する。そして、決済要求電文が受信されステップS41の判定が「Y」となると、ステップS42で認証処理を行う。この認証処理では、上述したように、受信した決済要求電文の署名確認及びユーザIDの確認を行うと共に、データベース42内に格納されているこの端末11Aの最終履歴データと、この受信電文

## 6

に含まれる最終履歴データとの間の一致の有無が確認される。

【0019】そしてこれらの確認結果が何れも正常でステップS43の判定が「Y」となると、ユーザ端末11Aによる種々の電子商取引に基づく決済処理をステップS44で実行し、その処理結果の残高情報に自身の電子署名を付加してデータベース42内のユーザ端末11Aに対応したファイル領域に最終履歴データとして記録する。その後、ステップS45でその最終履歴データを決済結果電文として該当ユーザ端末11Aに送信しそのファイル12Aを更新させる。

【0020】一方、ステップS42の認証処理の結果、異常となりステップS43の判定が「N」となる場合は、その異常が電子署名或いはユーザIDの不一致による異常か否かをステップS46で判断し、電子署名或いはユーザIDの不一致による異常の場合は、ステップS47でそのユーザID等をデータベース42内の別途領域に設けたブラックリストに登録し、以降の使用を禁止させる。

【0021】電子署名或いはユーザIDの不一致による異常ではない場合は、ユーザ端末12A側の履歴データと管理センタ14側の履歴データの不一致ということで、ステップS48で履歴データ不一致処理を実行する。その結果、第三者によりファイル12Aの内容がコピーされることによって無断で使用される等、ユーザA側でその理由が不明な場合はそのファイルを用いた取引停止の処理を直ちにステップS49で実行する。

【0022】また、ユーザファイルの破損や紛失等、ユーザAがその理由がわかっている場合については、上述したようにバックアップファイルの履歴データをユーザ端末12Aから管理センタ14へ送信する等の処理を行う。その結果、ステップS50で管理センタ14から最新履歴データをユーザ端末12Aに返送する等の処理を行うことにより、ユーザファイル12Aの更新が行われ以降のそのユーザファイル12Aを用いた取引が再開される。

【0023】このように、ネットワークを介した電子商取引における決済時には、ユーザファイル12内の最終履歴と、管理センタ14内の最終履歴との一致を確認することにより、その決済を許容するため、電子商取引を行う場合にその利用者を限定することができ、従って高セキュリティを確保できる。また、ユーザファイル12の破損や紛失等の場合は、バックアップファイルの履歴データをユーザ端末12から管理センタ14へ送信することにより、管理センタ14から返送される最終履歴データを受信しユーザファイル12の内容を更新する。この結果、以降そのユーザファイル12を使用して決済を行うことができる。

【0024】

【発明の効果】以上説明したように本発明によれば、電

子商取引に伴う決済時に端末はユーザファイルの最終履歴情報を管理センタに送信し、管理センタはこのユーザファイルの最終履歴情報とデータベースの最終履歴情報とが一致するときに決済を許容するようにしたので、電子商取引を行う場合に利用者を限定することができ、従って高セキュリティを確保できる。また、予めバックアップファイルを端末に設けて取引履歴情報をバックアップすると共に、管理センタからユーザファイルの最終履歴情報とデータベースの最終履歴情報との不一致が通知された場合、端末はバックアップファイルの取引履歴情報を管理センタへ送信しユーザファイルを更新するようにしたので、ユーザファイル内の履歴データの紛失や破損等が生じた場合でもこれを復旧して決済を行うことができる。また、管理センタは履歴情報に自身の署名鍵を用いて電子署名を行い端末へ送信してユーザファイルに記録させ、端末はユーザファイル内の履歴情報に自身のIDを付加すると共にIDが付加された履歴情報に自身の署名鍵を用いて電子署名を行い管理センタへ送信し、履歴情報の正否を検証させるようにしたので、電子決済

システムにおいてより高度なセキュリティ性を確保できる。

【図面の簡単な説明】

【図1】 本発明を適用した電子決済システムの構成を示すブロック図である。

【図2】 上記システム内のユーザファイルの構成を示す図である。

【図3】 上記システムの第1の動作例を説明する図である。

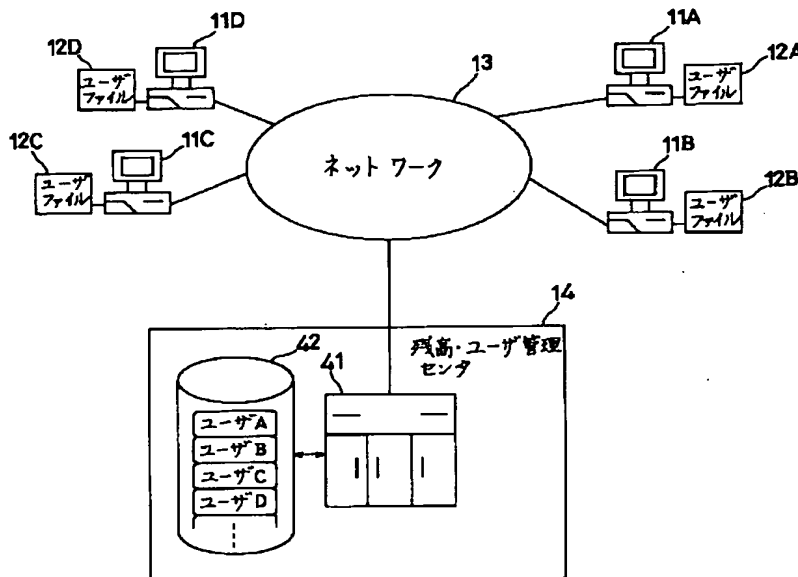
【図4】 上記システムの第2の動作例を説明する図である。

【図5】 上記システムの要部動作を示すフローチャートである。

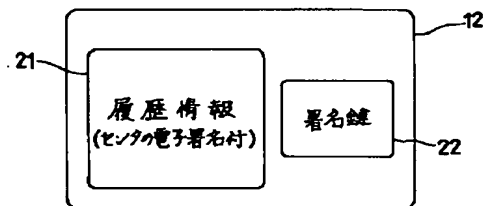
【符号の説明】

11A～11D…ユーザ端末、12A～12D…ユーザファイル、13…ネットワーク、14…残高・ユーザ管理センタ、15B…バックアップファイル、21…履歴情報、22…署名鍵、41…管理装置、42…データベース。

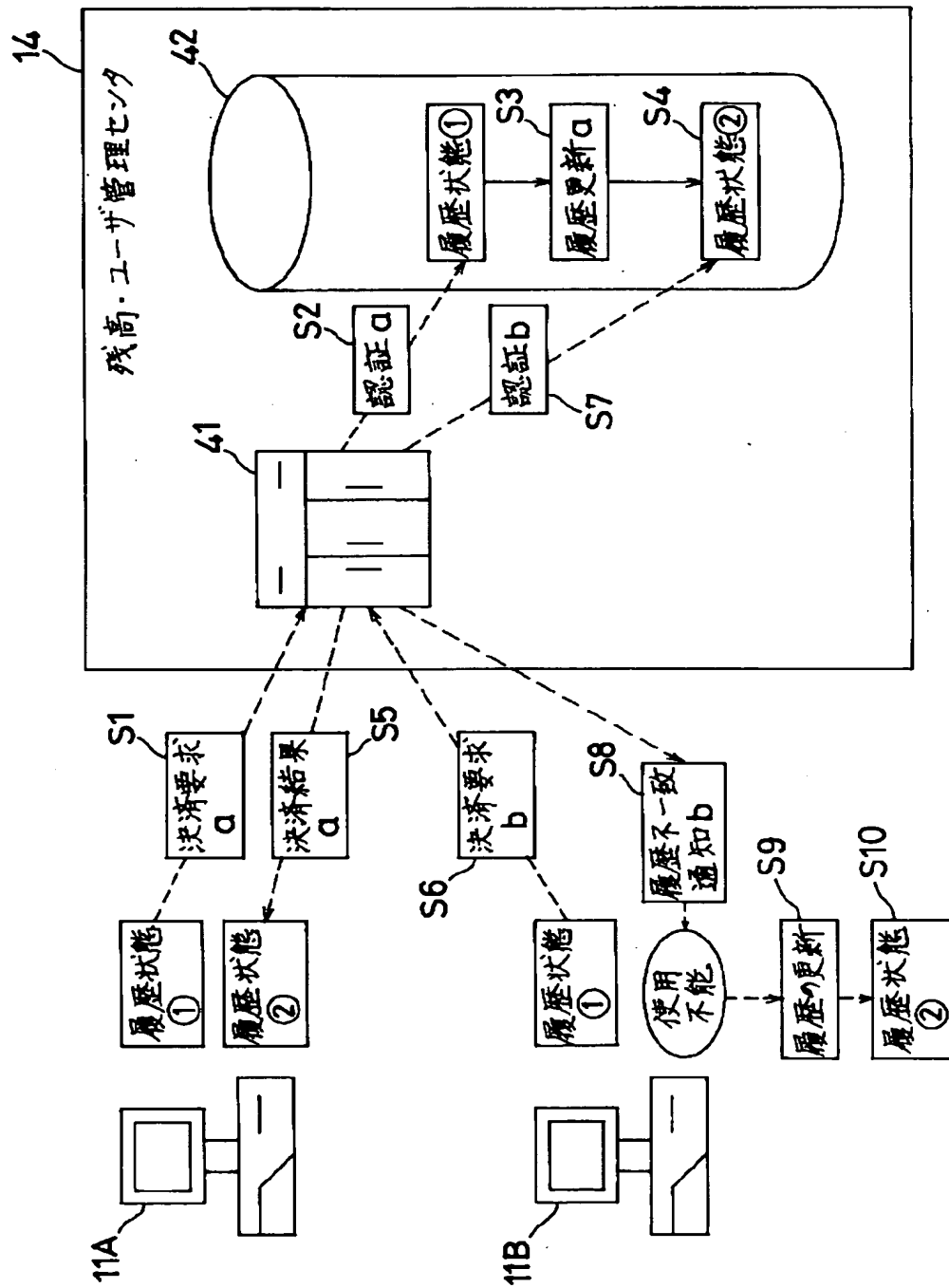
【図1】



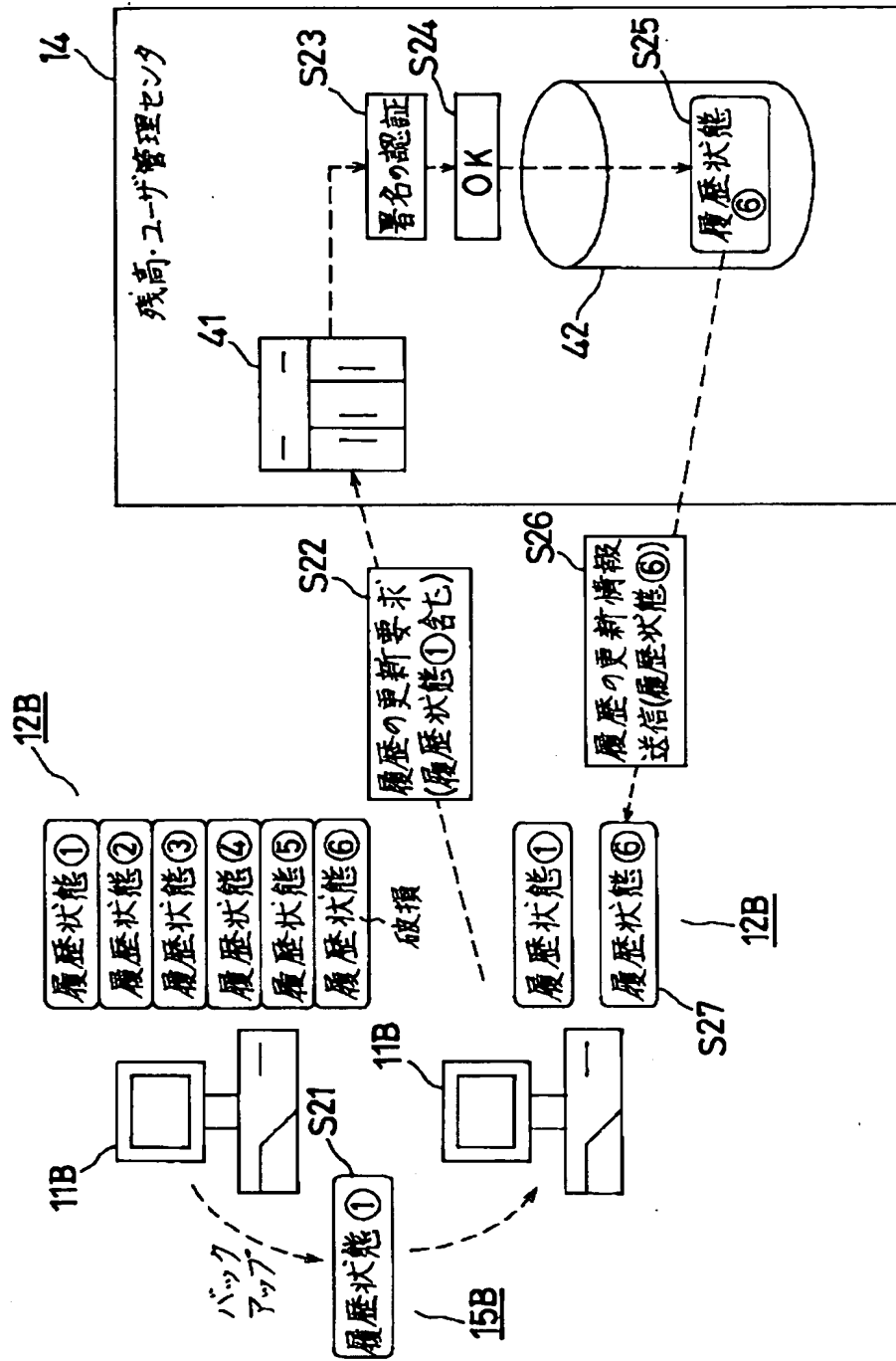
【図2】



【図3】



【図4】





【図5】

